THE BYOD DILEMMA:
HOW TO KEEP YOUR ASSETS FROM TURNING INTO LIABILITIES

WHITE PAPER

THOMSON REUTERS™

MITIGATING RISKS OF EMPLOYEE DEVICES

Author Daniel Garrie examines the benefits and risks of “Bring Your Own Device” policies

Benefits of BYOD

Personal smart phones dominate the corporate workplace. The BYOD, or “Bring Your Own Device,” has become ubiquitous in offices worldwide. One device for work and one for personal use is typical in today’s arena; it is more than just the social media marketing managers and savvy employees or lawyers who want continuous access. As employees look for more room to adjust hours and scheduling, BYOD allows them to easily bring work to home – and home to work.

Companies save money by lowering infrastructure costs and have the comfort of knowing that their employees have all their emails, files, and calendars in one place (or stored in the cloud and accessed from multiple devices) accessible at any time, increasing productivity and efficiency. The downside is that the individuals responsible for securing the workplace environment are gritting their teeth. Why? According to the Ponemon Institute, about 68 percent of respondents reported that their mobile devices have been targeted by malware of some variety during 2013. A survey published in the 2013 Summer/Fall issue of the Journal of Law & Cyber Warfare of more than 50 percent of the 300 senior executives at large and small companies stated they did not have a formal policy in place or the capability to manage employee-owned mobile devices. Below, we discuss the impact that not having policies and procedures in place to address BYOD issues can present for companies and law firms, big and small.

THREAT #1: A malicious viruses attacks a company systems by way of an employee’s mobile phone

On average, most employees, whatever their field, are not particularly malware savvy, which means they are not up on the details of evaluating security on apps that they download. Typically these individuals do not have malware scanning technology on their mobile devices. Many companies today invest substantial resources in providing employees with robust anti-virus and malware scanning tools for their computers and information systems, but leave the employees mobile devices exposed and vulnerable to thousands of potential adversaries.

How, then, to protect against these potentially disastrous smartphone malware-laden apps? Most companies purchase anti-virus, anti-malware software for their computers. It seems logical, then, to extend that policy to mobile devices as well. Why not invest in protecting your employees’ devices? By extension, protecting employee devices provides insurance for the security of a company.

People bring their devices to work whether or not there is a stated policy in place, and whether or not they are able to actually do work on those devices. One solution is to mandate that every mobile device used by employees must have malware detection software installed.   Of course, the solution is likely to require that a lawyer skilled in these issues review the policies, the underlying software agreements, and the privacy agreements involved with

Daniel B. Garrie is a partner at Law and Forensics.com, where he focuses on e-discovery and forensics and acts as Special Counsel to the law firm of Zeichner Ellman & Krause, specializing in e-discovery and cyber-security matters.

implementing this solution. It is critical that the lawyer advising any company has a firm grasp of the complex legal issues and the technologies to ensure a successful rollout.

Recommendation: Purchase mobile malware detection software and require employees to have this software installed and operational on their mobile devices

THREAT #2: Malware compromises mobile device and then jumps to corporate systems wreaking havoc

An employee owned android device ends up getting infected with malicious malware over the weekend and the unknowing employee brings the device to work on Monday. Unfortunately, one infected phone, in an unsecured BYOD workplace, can serve as a vector of malware to the entire corporate network, as well as other BYOD devices.

Malware can spread onto the network and infect multiple computers within the system, potentially stealing data, compromising systems, and crippling businesses until they are able to eradicate the issue. One possible solution is for a company to mandate malware protection software on every device. Again, it is critical that the lawyer advising any company has a firm grasp of the complex legal issues and the technologies to ensure a successful rollout.

Recommendation: Purchase mobile malware detection software and require employees to deploy malware software on any mobile device used in the workplace

THREAT #3: An employee's mobile device Is lost or stolen and ….

The third risk seems very low-tech, but it is in some ways the greatest threat. When a phone is lost or stolen, unless the phone's owner has subscribed to a service that allows remote locking or wiping of the phone's memory, it may come equipped with everything from that person's bank account details to their work computer logins, emails, legal files, family photos, and the list goes on.

Unfortunately, most corporate cultures tend to penalize employees when mobile devices are lost or stolen often creating a several day gap as the employee frantically attempts to find the mobile device, relying on the passcode as a barrier. The reality is that today, a passcode key is no barrier. Often a user need only look at the marks on a screen to replicate a swipe pattern or go on-line and download one of the many tools available for free to hack a mobile phone.

There is no magic bullet here to solve this issue and often the solution will vary based on geography, size, culture, industry, technologies, and many other factors. One possible solution is to mandate that all mobile devices used in the workplace have robust encryption.

Another solution is to review and amend existing mobile application(s) and BYOD policies to allow your IT department to track the devices and wipe remotely in certain situations. By incorporating asset tracking into the policy the company will be able to track any device brought into the workplace allowing employers to ensure malware detection software is appropriately installed and updated, as well as, keep track of devices that are potentially carrying proprietary/sensitive information. An employer, by obtaining the "right to wipe," can avoid potentially expensive legal disputes and respond quickly in the event of a lost or stolen device, assuming that this is permissible in the countries within which you operate. In certain countries there is a constitutional right or culture of privacy that may make implementing such a policy challenging. Here, it is critical that the lawyer advising an organization has a firm grasp of the company culture, the underlying legal issues, the technologies, and the real-world experience in this area of the law.

Often overlooked, but an effective solution is to create a corporate culture that allows for pseudo anonymous reporting, meaning that if a device is lost or stolen, an employee must be able to report the loss without fear of punishment or repercussions. This allows the company to proactively deal with the potential problem and the employee is able to get a new device, a win-win dynamic.

Recommendation: Implement encryption. Adjust company BYOD policy to allow for asset tracking and remote wiping. Implement a pseudo anonymous reporting policy framework for lost or stolen device.

CONCLUSION

As we look forward into 2014, law firms and companies, big or small, must develop, implement, and deploy BYOD policies that suit their culture, geography, security, and confidentiality needs.

"Malware can spread onto the network and infect multiple computers within the system, potentially stealing data, compromising systems, and crippling businesses until they are able to eradicate the issue."

We suggest several possible solutions, including: mandatory registration of any device that enters the professional workspace; installation of approved malware detection software on every such device, which should include the ability to remotely wipe a device's internal storage; anonymous or no-penalty reporting of loss of devices; and the company's right to wipe said devices in such an event.

Law firms and companies may be hesitant to rock the boat and risk potential backlash that can arise when privacy becomes the focal point of the conversation. While such concerns in certain context can be well founded, it is often not the case. Employers must work to create an environment where employees know that the tools and policies around BYOD are not being used to spy or invade on personal lives, but are being used to protect both the employee and the employer. One thing is for sure: BYOD is here to stay and organizations, big and small, should work proactively to protect themselves.

Daniel Garrie has published over 100 articles, is recognized by several Supreme Court Justices for his legal scholarship, and is the Editor-in-Chief of the Journal of Law and Cyber Warfare. Mr. Garrie is co-author of two titles published by Thomson Reuters: the new title *Plugged In: Guidebook to Software and the Law* and *Dispute Resolution and e-Discovery*, published in 2011. Mr. Garrie is admitted to practice law in New York and New Jersey.